Secure MIMO Visible Light Communication System Based on User's Location and Encryption

Farag Mousa, Noor Almaadeed, Krishna Busawon, Ahmed Bouridane and Richard Binns

***Abstract*—Visible light communication systems are rapidly growing research areas with wide applications ranging from illumination and data communication. To achieve high data rates in such systems, a number of techniques have been employed such as equalization of transmission signals, deployment of complex data modulation and the use of multiple input multiple output (MIMO) systems. However, security in wireless telecommunication systems is a common concern. This paper proposes a secure MIMO-VLC system that relies on the position of the user by incorporating a new modified version of the Rivest-Shamir-Adleman (RSA) technique for encrypting the transmitted data in the Media Access Control (MAC) layer. The performance of the positioning method is evaluated showing a positioning accuracy of less than 5cm for a signal-to-noise ratio (SNR) of 15 dB. Furthermore, the ability of the proposed system to control the size of the encrypted cell, depending on the application environment, is demonstrated.**

***Index Terms*—Light Emitting diodes; Received signal strength indication; Localization; Indoor positioning; Visible Light Communication system; Trilateration method; Cryptography; Encryption; Decryption; RSA algorithm; Encrypted cell; MIMO; VLC.**

I. Introduction

In recent years, visible light communication (VLC) systems have emerged as a new and competitive technology in optical wireless communication (OWC), gathering significant research attention [1]. A VLC system provides two functions: one is lighting in indoor environments, and the other is wireless data communications [2]. In addition, it offers high security, high data rates, and precise positioning detection compared with other wireless communication systems [3]. The high data rates can readily be exploited to create optical multiple-input-multiple-output (MIMO) communication systems. MIMO techniques have been applied in many radio frequency (RF) systems to increase the throughput by increasing the spectral efficiency [4] as well as to make the transmission more robust without increasing the data bit rate. MIMO-VLC systems have thus become an attractive approach for increasing the channel capacity, particularly in an indoor environment. Such systems have already been demonstrated to achieve Gbps data rates and been reported in [5]–[7]. There are two main categories for a MIMO-VLC system: (a) imaging MIMO which is similar to a camera communication technique, which requires an optical subsystem. (b) Non-imaging MIMO which is a simpler and more robust technique against mobility conditions and employs multiple transmitters and receivers to accomplish parallel data transmission. The receiver can receive data separately if it has full knowledge of the channel-state information (CSI) from the transmitting pilot signals (PS). The main contributions of this paper are three fold and can be summarized as follows: (i) development of a mathematical modelling of positioning in MIMO-VLC systems, (ii) design of novel secure MIMO-VLC system based on user's location and encryption without affecting the efficiency in both ideal and real scenarios and (iii) deployment of encryption at the MAC layer with no overhead data and with the ability to control the size of the encrypted VLC cells based on the user environment.

The rest of this paper is structured as follows: Section II gives some preliminaries on MIMO-VLC, positioning, and cryptography. Section III presents the positioning in MIMO-VLC system using the RSSI technique and the trilateration method. Subsequently, section IV presents the secure MIMO-VLC system description. The simulation setup, BER distribution and a discussion are presented in section V. Finally, a conclusion is given in section VI.

Farag Mousa, Krishna Busawon, Ahmed Bouridane and Richard Binns are with the Faculty of Engineering and Environment, Northumbria of University, Ellison Building, Newcastle Upon Tyne, UK, NE1 8ST, e-mail: farag.mousa@northumbria.ac.uk.

Noor Almaadeed is with Department of Computer science and Engineering, Qatar University, Doha, Qatar, P.O. Box: 2713.

Manuscript received .....; revised .....

II. Problem Statement and Review of MIMO-VLC, Positioning, and Cryptography

A. MIMO-VLC System

1) The considered MIMO system model: An optical MIMO-VLC transmission system employs four transmitters (4-LED array) through intensity modulation and direct detection (IM/DD) with four independent and simultaneously transmitted data streams using multiple incoherent light sources and photodetectors as shown in Fig. 1 (a). The number of transmitters and/or receivers in the system can be increased or decreased depending on the size of the location and the illumination footprint requirement without affecting the MIMO principle. In this paper, the receiver's body consists of four photodetectors (PD) (with optional non-imaging concentrators). The receivers collect the light from transmitters, estimate the channel matrix and recover the original data using MIMO signal processing. Fig. 1 (b) describes a 4×4 MIMO-VLC system. The input binary stream data is sent to the serial to parallel converter. The converter subsequently supplies outputs that are parallel data streams, which are then DC-level shifted and intensity modulation through the LED transmitter Tx_j. The transmitted signals are x_j where j is 1,2,...M and

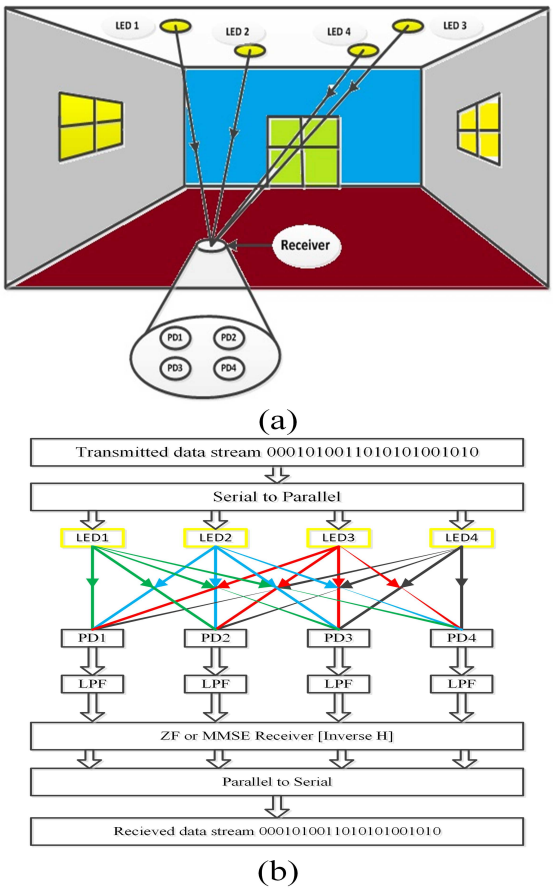


Fig. 1: (a) A 4x4 MIMO-VLC system (b) The block diagram of a 4x4 MIMO-VLC system

M is the number of LEDs at the transmitter side [4], [8], [9]. All data streams are transmitted simultaneously. Every receiver will receive a signal which is a linear combination of all x_j. The retrieve process of the transmitted data from multiple signals involves estimating the channel coefficients between each transmitter Tx_j and receiver Rx_i. These channel coefficients are called the CSI matrix (H matrix) and also called the transmission matrix. In other words, h_{ij} denotes the channel gain for the i^{th} and j^{th} channels between each pair of Tx_j and Rx_i, where j is the number of PDs at the receiver side. The conventional model for MIMO-VLC system can be expressed by

$$y = Hx + n \tag{1}$$

where, y is the received signal vector, H is the channel matrix, x is the transmitted signal vector and n is the additive white Gaussian noise (AWGN) vector. Equation (1) can be further expanded as follows:

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & h_{13} & h_{14} \\ h_{21} & h_{22} & h_{23} & h_{24} \\ h_{31} & h_{32} & h_{33} & h_{34} \\ h_{41} & h_{42} & h_{43} & h_{44} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{bmatrix} \tag{2}$$

2) H-matrix: The channel coefficient is denoted by h_{ij} which originates from the j^{th} transmitter to the i^{th} receiver $(1 \leq i, j \leq M)$. In this paper, we consider that the dominant link configuration between Tx_j and Rx_i is the line-of-sight (LOS), and as such, h_{ij} is defined as the DC channel gain and expressed by:

where θ_{ij} is the irradiance angle, ψ_{ij} is the incidence angle, $T_s(\psi_{ij})$ is the gain of an optical filter, $g(\psi_{ij})$ is the gain of an optical concentrator, A_R is the detector's effective area, d_{ij} is the transmitter-to-receiver distance and m is the Lambertian emission which is expressed as:

$$m = \frac{-\ln(2)}{\ln(\cos(\theta_{1/2}))} \tag{4}$$

where $\theta_{1/2-j}$ is the semi-angle at half luminance of the j^{th}LED and FOV_i is the field of view of the receiver [1], [10].

3) MIMO receiver: To cancel the effect of the channel matrix (H) at the receiver side, we transform the received signal vector (Y) using a matrix equaliser to obtain the estimation of the transmitted signal vector (X). There are a number of criteria that can be used to estimate the channel coefficients [11], The Zero-Forcing (ZF) equaliser was proposed by Robert Lucky as a low complexity linear equaliser and , as its name indicates, acts to minimize the ISI to zero and give a flat frequency response and a linear phase from the combination of the channel characteristics and the equaliser [12]. However, this equaliser has its disadvantages, as it requires an accurate channel state information (CSI) to achieve a proper operation and suffers from noise amplification. To overcome this drawback, a Minimum Mean Squared Error (MMSE) equaliser is proposed as a solution and is discussed in next subsection.

a) MMSE Equaliser:: In this technique, the squared error of a random variable is first performed after which a mean is taken. This value represents a very critical difference in statistics and is known as a Bayesian approach useful to treat the transmitted symbol vector in the mean domain. The MMSE equaliser is a linear equaliser, and it is also known as an optimal detector because it works to alleviate ISI and reduce the noise as well. The mathematical model of the MMSE equaliser is given as:

$$\widehat{x} = argmin\{E\left\|\widehat{x} - x\right\|^2\} \tag{5}$$

$$= argminE\left\{\left\|\overline{C}^T\overline{y} - x\right\|^2\right\} \tag{6}$$

Then, the equaliser matrix is given as:

$$\widehat{c} = P_d\left(P_d HH^T + \sigma_n^2 I\right)^{-1} H \tag{7}$$

where, P_d and σ_n^2 are the powers of the transmitted signal and the noise at the receiver, respectively. Finally, the linear MMSE equalizer for the MIMO system is given as,

$$\widehat{x} = P_d\left(P_d HH^T + \sigma_n^2 I\right)^{-1} H\overline{y} \tag{8}$$

for the real channel matrix and

$$\widehat{x} = P_d\left(P_d HH^H + \sigma_n^2 I\right)^{-1} H\overline{y} \tag{9}$$

for the complex channel matrix. The above equation can be written as:

$$\widehat{x} = \left(HH^H + \frac{1}{snr} I\right)^{-1} H\overline{y} \tag{10}$$

$$h_{ij} = \frac{(m+1)}{2\pi d_{ij}^2} A_R \cos^m(\theta_{ij}) \cos(\psi_{ij}) T_s(\psi_{ij}) g(\psi_{ij});\ \text{if } 0 \leq \psi_{ij} \leq FOV_i \tag{3}$$

where, $snr = \frac{P_d}{\sigma_n^2}$. Here, at high SNR, the MMSE equalizer approaches to ZF equalizer [13]. The aim of this work is to investigate and implement a secured MIMO-VLC system. The main idea with this kind of system is to use traditional cryptography techniques that rely primarily on the user's location to achieve the security of the VLC links.

B. Positioning in VLC system

There exit a number of techniques for the positioning of indoor systems including methods using LEDs that have been employed in Wi-Fi networks. One of these techniques is based on time difference of arrival of pulses (TDOA) where the difference of arrival times between signals at multiple transmitters is used to determine the relative position of the user [14], [15]. The second technique is based on the angle of arrival (AOA) and uses the angle from which a signal arrives at a receiver, where the target location in 2D is determined using only two known reference points and two measured angles [16]. The third technique is known as the time of arrival (TOA); that is the aggregate of time to transmit the signal from the user's location [17]. The last but not least technique is based on the received signal strength indication (RSSI). This method measures the power levels received from each transmitter separately, and then estimates the distance between the receiver and the transmitter based on the relationship between the transmitted (P_{Tx}) and received (P_{PD}) signal strength as follows:

$$P_{PD_j} = P_{Tx_i}.h_{ij}(L).G_r \tag{11}$$

where; $h_{ij}(L)$ is the channel gain, L is the distance between the transmitter and receiver, G_r is the receiver gain [18]. We use the RSSI technique of indoor positioning using three transmitters with the trilateration method. The method recovers the channel characteristics from incident light and estimates the receiver location by analytically solving the Lambertian equations.

C. The RSA Technique

Several studies investigating RSA algorithm have been carried out on the improvement of security and overcome the limitation in RSA algorithm. Fig. 2 shows the block diagram of public-key cryptosystem to provide secrecy. The limitations in RSA algorithm are the speed of implementation, computational cost, loss of private key sometimes results to break the security and some types of attacks for example factorization problem or short message. The RSA security depends on the large prime numbers but they are easily factored and decomposed [19]. Wuling Ren and Zhiqian Miao have implemented a novel approach based on DES and RSA algorithms in Bluetooth Communication using DES and RSA

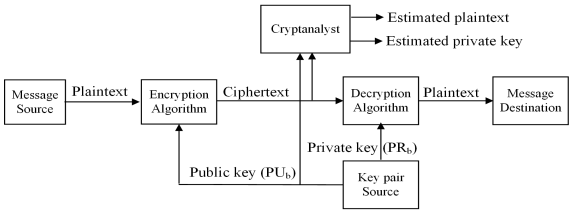


Fig. 2: Public-key cryptosystem to provide secrecy

algorithm to encrypt transmitting data and keys, respectively [20]. In [19], a new RSA algorithm by Sonal Sharma et al, which uses modified Sum Cryptosystem based on a subset sum of two numbers over RSA public key. B. Persis Urbana Ivy et al. have used N numbers to generate public and private keys. That are not easily decomposed or factorized to getting high security and efficiency through a network [21].

1) Key Generation Process: In RSA, public and private keys are generated by a series of mathematical steps as follows:

- Generate two large different prime numbers p and q
- Compute $n = pq$
- Compute the Euler Totient Function: $f(n) = (p-1)(q-1)$
- Select a random the encryption key e, where $1 < e < f(n)$, $gcd(e, f(n)) = 1$
- Calculate the private exponent value for the decryption key d such that $d = (e-1) mod f(n)$
- Public key = $[e, n]$ and private key = $[d, n]$ [22].

2) Encryption/decryption: The transmit message $m_t (0 = m_t < n)$ is encrypted by the public key at the sender by applying following expression [23]–[27]:

$$C = m_t^e mod(n) \tag{12}$$

At the receiver, the original message is recovered by:

$$m_r = c^d mod(n) \tag{13}$$

III. The Proposed Positioning in MIMO-VLC System

A. Mathematical model

The following discusses our proposed model based on the principle of calculating the path loss as a result of attenuation. From (3) and (11), which are basic equations, can calculate power distribution in a VLC environment for any location inside a room. The received optical power at a distance L utilizing (14) with the assumption of $\psi_{L_{ij}} = \theta_{L_{ij}}$ can be expressed as: Thus, the received optical power underneath the transmitter, i.e. at a distance h as shown in Fig. 3 ($\psi_{L_{ij}} = \theta_{L_{ij}} = 0$), is given as:

$$P_{PD,h_j}(\theta_{ij},\psi_{ij}) = P_{Tx_i}\frac{(m+1)}{2\pi L_{ij}^2}.\cos^m(\theta_{ij})\cos(\psi_{ij}).T_s(\psi_{ij})g(\psi_{ij}) \tag{14}$$

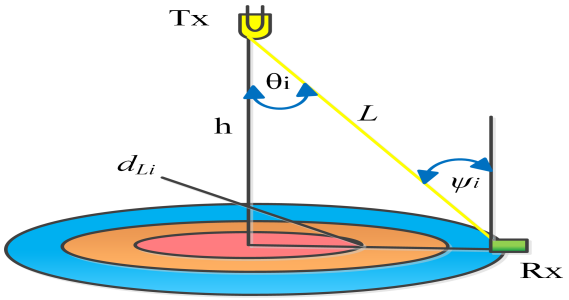


Fig. 3: Side view of 1-D indoor MIMO-VLC system

$$P_{PD,h_j} = P_{Tx_i}\frac{(m+1)}{2\pi h_j^2}. \tag{15}$$

From (14) and (15), assuming $T_s(\psi_{ij})g(\psi_{ij}) = 1$, meaning that we do not have any attenuation or amplification for the received optical signal from these stages because of the employed positioning VLC technique here is RSSI technique which is depended on the received power level as well as $L_{ij} = \frac{h}{\cos(\theta_{ij})}$, the mathematical model of RSSI technique can be written as:

$$P_{PD,L_j}(\theta_{ij}) = P_{PD,h_j}(0).\cos^{(m+\gamma+1)}(\theta_{ij}) \tag{16}$$

where $i = j = 1, 2, 3$ or 4 represents the number of transmitter and the number of photodetectors in the room and $\gamma = 2$ is a path-loss exponent correction factor [18], [22].

B. Horizontal Distance Estimation

From (16) one can measure the angle of irradiance ($\theta_{L_{ij}}$) using measurements of the received power at a distance h ($P_{PD,h_j}(0)$) and store it at the receiver which uses it along with the received power at distance L_{ij} for all positions in the room. The final step calculates the horizontal distance estimation using simple trigonometry [22]:

$$d_{L_{ij}} = h.\tan\theta_{ij} \tag{17}$$

C. Trilateration method

The process of locating absolute or relative locations of targets by measuring the distances using the geometry of circles is shown in Fig. 4. As the figure illustrates, there are four power levels to be measured at the receiver side. However, the receiver will select only the three maximum power levels that will be used in the positioning algorithm in order to determine the location of the user. So, we can use the RSSI algorithm to calculate θ_{ij} (i.e., θ_{1j}, θ_{2j} and θ_{3j}) and then calculate $d_{L_{1j}}$, $d_{L_{2j}}$ and $d_{L_{3j}}$ using (16) and (17) respectively. Now, the trilateration method can be used to determine the position of user by obtaining the intersection point from the three following equations;

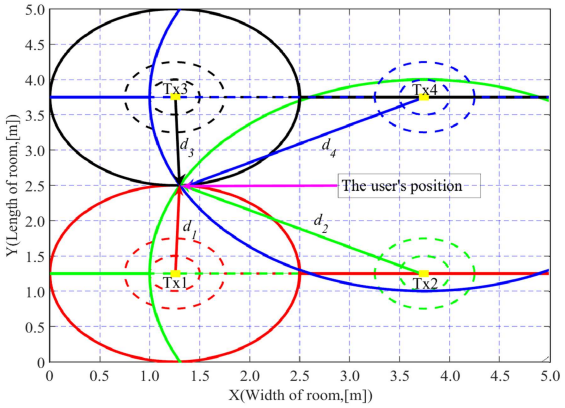


Fig. 4: Top view of 2-D system for positioning system using trilateration method

$$\begin{cases} (x_{PDj}-x_{Tx_1})^2+(y_{PDj}-y_{Tx_1})^2 = d_{L_{1j}}^2 \\ (x_{PDj}-x_{Tx_2})^2+(y_{PDj}-y_{Tx_2})^2 = d_{L_{2j}}^2 \\ (x_{PDj}-x_{Tx_3})^2+(y_{PDj}-y_{Tx_3})^2 = d_{L_{3j}}^2 \end{cases} \tag{18}$$

where $d_{L_{1j}}^2$, $d_{L_{2j}}^2$ and $d_{L_{3j}}^2$ are the horizontal distances between the LEDs and PDs and (x_{Tx_1}, y_{Tx_1}) , (x_{Tx_2}, y_{Tx_2}) and (x_{Tx_3}, y_{Tx_3}) are position coordinates of the transmitters; while (x_{PD_j},y_{PD_j}) is the coordinates of the photodetector in the receiver array [24].

D. CORA calculations

The receiver array has two different designs based on the directional order of photodetectors as shown in Fig. 5. There are two configurations for designing the receiver array: (i) anticlockwise configuration (ii) clockwise configuration. If the coordinates of each of photodetector 1 (x_{PD_1}, y_{PD_1}) and photodetector 2 (x_{PD_2}, y_{PD_2}) are known, we can calculate the coordinates of both photodetectors 3 and 4 (in an anticlockwise configuration) from the following expressions:

$$x_{PD_3} = x_{PD_2} \quad \text{and} \quad y_{PD_3} = y_{PD_2} + \Delta y \tag{19}$$

$$x_{PD_4} = x_{PD_1} \quad \text{and} \quad y_{PD_4} = y_{PD1} + \Delta y \tag{20}$$

Note that in this proposed system, the requirement is to calculate the coordinates of the centre of the receiver (CORA) and not the coordinates of each photodetector in the receiver array. The estimation of the coordinates of CORA can be calculated using the following equations to reduce the positioning error:

$$x_{CORA} = \frac{1}{N}\sum_{J=1}^{N}\left(x_{PD_j} + \begin{cases} \frac{\Delta x}{2} & \text{if} \quad \text{j = 1, 4} \\ -\frac{\Delta x}{2} & \text{if} \quad \text{j = 2, 3} \end{cases}\right) \tag{21}$$

$$y_{CORA} = \frac{1}{N}\sum_{J=1}^{N}\left(y_{PD_j} + \begin{cases} \frac{\Delta y}{2} & \text{if} \quad \text{j = 1, 2} \\ -\frac{\Delta y}{2} & \text{if} \quad \text{j = 3, 4} \end{cases}\right) \tag{22}$$

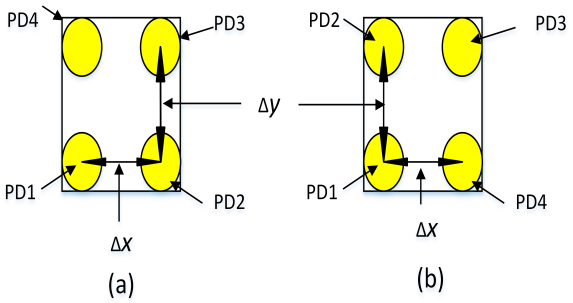


Fig. 5: The receiver array (a) anticlockwise configuration (b) clockwise configuration

IV. Secure MIMO VLC system description

The security task in wireless communications has become a matter of concern due to the possibility of unauthorised access to transmitted data. This stems from the fact that all users use the same channel. However, in a VLC system, this issue is less pronounced because of the inability of light to through the walls. Recently, several types of research have been proposed on security at the physical layer to encrypt the user's data [30], [31]. A typical MIMO-VLC system is designed to broadcast signals and hence any user in the VLC cell range can receive the transmitted data inside the illumination coverage area. This communication system does not have a secured transmission link for each user.

A. Block diagram of secure system

Figure 6 shows the block diagram of the proposed end-to-end secure MIMO-VLC system [28], [29]. It consists of a transmitter and a receiver, as well as 4×4 MIMO-VLC channels acting as the downlink and an RF or IR channel acting as the uplink due to the VLC system not possessing an uplink. This still presents the biggest challenge in VLC systems, and as such an RF/IR uplink was adopted. At the transmitter side, there is a coordinator that has the location codes of the transmitters' positions.

In case I: the user is new, the coordinator sends locations codes only to receiver via the MIMO-VLC channel [28], [29]. The receiver receives four signals using four photodetectors and recovers data by the MMSE equaliser. In the next stage, it calculates the user's location based on the RSSI technique that has been discussed in the previous section. The receiver can select the public and private keys from keys' store based on its location, and then sends the public key and power levels to the transmitter via the RF/IR channel. The transmitter subsequently receives them, and decides if the MIMO-VLC channel is suitable for data transmission.

In Case II: the coordinator encrypts the user's data utilizing the public key and combines them with the location codes and sends the data via the MIMO-VLC channel. At the receiver side again, all four signals pass the photodetectors stage, the positioning stage and finally the decryption process using the private key to decrypt the data. In positioning stage, if the new location is not the same as the previous one, the receiver generates another key based on the new location using the cryptographic keys stage.

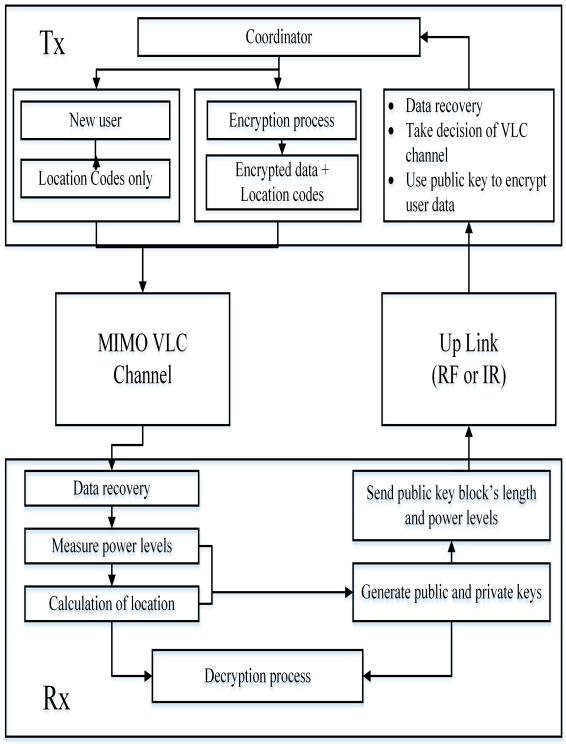


Fig. 6: Bock diagram of secure MIMO-VLC system

B. Modified RSA algorithm and encrypted cells

In Fig. 6 there is a stage at the receiver side that generates public and private keys. In this section, we explain the modified RSA algorithm that produces a number of encryption/decryption keys and distributes them on encrypted VLC cells. All frames from the transmitted data are divided into k-bits parallel blocks (k = 8, 16, 32, 64, ...), where k is chosen to be the same length as the key, which is generated by this modified RSA algorithm. The modified RSA algorithm is given in *Algorithm 1* below. We have modified the RSA algorithm for two main reasons; the first is the need to encrypt data without an increase in data length compared with plaintext data and as such to maintain the capacity of the channel. This means that the transmitted message per block $m_t(i)$ must not be more than n ($0 \leq m_t < n$). For instance, if we have a block of 8 bits that means n must be less than 255. However, there is a difficulty to find two prime numbers (p and q) of which their multiplication result is exactly equal to m. Therefore, we select a percentage which is called maximum percentage of unencrypted data (MPUED) between data that is encrypted and data that cannot be encrypted (because it is more than n). The second reason is the requirement to generate a number of keys that are enough for every encrypted VLC cell. In the modified RSA technique, we are adding another level of ambiguity by not encrypting all transmitted data that is less than five percent. In this secure system, the problem of keys distribution has been solved using the generation of cryptographic keys in receiver (i.e.; at user) and sending the public key to transmitter only [22], [23], [32]–[34]. The second process in this part relates to the distribution of keys on the

encrypted VLC cells. In Fig. 7 the standard VLC room has been divided into small square areas called the Encrypted VLC cells, where each encrypted cell has only one centre called the centre of encrypted cell (COEC). This means that every estimated user's location approaches the closest cell's centre due to the presence of a localization error based on positioning techniques and SNR. This approximation is the reason why it is difficult to make encrypted VLC cells smaller than this area. This system represents a flexible scheme in that it is able to control the size of encrypted cell. In Fig. 7, we have three sub-figures which show three different sizes of encrypted VLC cells. We have tested 4, 16 and 49 receivers for different lengths of cells, which are 0.50m, 1.00m and 1.50m, respectively. Therefore, all receivers in encrypted VLC cells have only COEC (i.e., all positions inside cell approaches to one position which is COEC), and then all receivers have the same identification but they will take different public and private keys. Therefore, if one reduces the size of encrypted cells then the number of receivers will decrease as well. For example, if we decrease the length of encrypted VLC cell from 1.5 m to 1.0 m, at that point then the number of receivers will decrease from 49 to 16 receivers as well. The reason being we have assumed different environments such as convention hall, large office having approximately 16 users and small office has around four users. In a convention hall, the LEC is assumed 0.5m because the number of users is large and close to each other and every user has two or three devices. In addition, these devices have the same COEC due to its deployment/use by one user. In proposal model, there will not be computational complexity because every receiver generates cryptographic keys based on its location and implements a decryption process as well.

- *Choose key's length* $m = 2^{k_l}$, $MPUED$
- *Generate prime numbers* $(P(:), Q(:)) \leq m$
- *Generate* $n(:) = P(:) * Q(:)$, $\phi_n(:) = (P(:) - 1)$ $(P(:) - 1)(Q(:) - 1)$
- $If\ n(i) \rangle m\ or$ $P(i) == Q(i)\ or\ n(i) \leq (n - MPUED)$ *delete* $P(i), Q(i)\ and\ \phi_n(i)$
- *Generate prime numbers less than* $\phi_n(:)$ *to get public key* $(e(:), n(:))$
- $If\ gcd(e(i), \phi_n(i)) == 1$ $e(:) \longleftarrow e(i)$
- *Generate prime numbers less than* $\phi_n(:)$ *to get private key* $(d(:), n(:))$
- $If\ e(i) * d(i) mod\ \phi_n(:) == 1$ $d(:) \longleftarrow d(i)$
- $If\ e(i) == d(i)\ or\ e(i) * d(i) == d(i) * e(i)$ $e(:) \longleftarrow e(i)\ and\ d(:) \longleftarrow d(i)$

Algorithm 1: Generation public and private keys based on block's length.

C. Encryption/Decryption in MIMO-VLC system

The receiver generates the public and private keys based on user's location, and sends the public key only to the co-ordinator at the transmitter side by the RF/IR uplink channel.

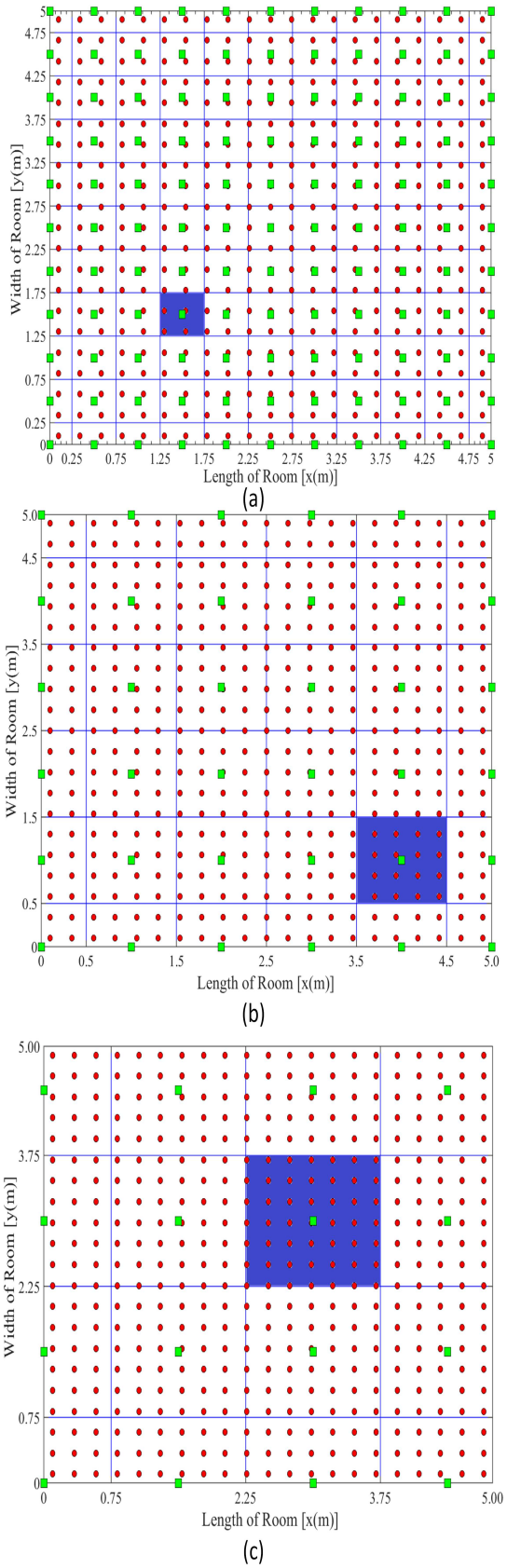


Fig. 7: The encrypted VLC cells with the centers of encrypted cells (COECs). Green square is COEC, red circles are the positions of the users, and blue square areas are examples of encrypted VLC cell size for different length of encrypted cell (LEC) (a) LEC=0.50m (b) LEC=1.00m and (c) LEC=1.50m.

TABLE I: The comparison between the RSA algorithm and the modified RSA algorithm

No.	The RSA Algorithm	The Modified RSA Algorithm
1	We must select p and q to determine common modulus n.	We have been calculated p and q based on encryption blocks lengths to get common modulus n.
2	The large prime number depend on only two variables p and q to provide the strength of the algorithm.	The strength of the algorithm is based on three variables p,q and k_l. Therefore, that is more difficult to break
3	All parameters and calculations to select and generate the p, q, e, and d are at the time of data transmission.	All parameters and calculations to generate the number of public and private keys with different blocks lengths are stored in database table in the receiver.
4	We have used (e, n) as public key and (d, n) as private key for encryption and decryption, processes, respectively.	We have used $(e(i), n(i), K_l)$ as public key and $(d(i), n(i), K_l)$ as private key for encryption and decryption processes, respectively.
5	We need to secure channel between Tx and Rx to exchange the keys, especially, private key.	We just need to send public key from Rx to Tx because the keys are generated in receiver side based on the position of the user.
6	The user has just one public key and one private key and are changed based on the time period where it is sometimes longer.	The user has a number of public and private keys and are changed based on the position of the user and from time to time as well.
7	The RSA algorithm is applied in application layer.	The modified RSA algorithm is applied in MAC layer.

The coordinator converts the data (the binary stream) into k-bits parallel blocks (k = 8, 12, 16, ...) based on the public key's length which is generated and transmitted by the receiver. These blocks are then converted into decimal values and encrypted using the RSA encryption formula:

$$C = m_t^{e(i)} mod(n(i)) \tag{23}$$

where ($e(i)$, $n(i)$, k_l) is the public key and m_t and C are the parallel transmitted and encrypted data, respectively. The parallel encrypted data is converted into serial data with an output in an OOK-NRZ format as shown in upper part of Fig. 8. The bottom part of the figure depicts a block diagram of the RSA decryption after recovering the original data signal. The receiver converts the data from serial into parallel blocks and applies the RSA decryption using the private key that already exists at the receiver side using the folowing formula:

$$m_r = c^{d(i)} mod(n(i)) \tag{24}$$

where ($d(i)$, $n(i)$, k_l) is the private key and C and m_r are the parallel encrypted and received data, respectively. In the final stage in the process, all decrypted parallel data are converted to decrypted serial data and passed through the upper layers. We have compared our modified RSA algorithm with RSA algorithm as shown in Table I.

V. Results and discussions

A. Test parameters

The proposed system described in the previous block diagrams of Fig. 6 and Fig. 8 is simulated and evaluated

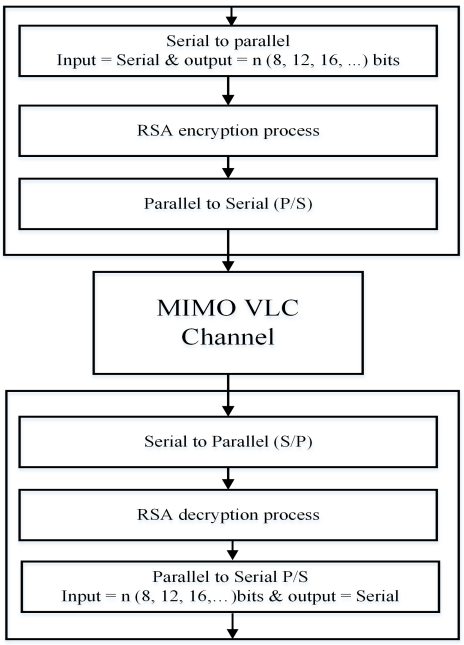


Fig. 8: The RSA encryption/decryption applied in MIMO VLC system

using MATLAB. The coordinator generates location codes depending on the transmitter's positions on the ceiling and combines them to the transmitting data signal $x(t)$ to be sent to the receiver by an LED. The transmitted signal is modulated utilizing an On-Off-Keying (OOK) modulation scheme. Each transmitter contains a number of LEDs whose parameters are similar to typical commercially LED devices. There are two types of noise associated with proposed system: thermal noise and shot noise. In this paper, we have calculated the transmission matrix (CSI) from (3) which is then used to find y matrix from (2). Furthermore, at the receiver side, the transmission matrix is available and we have used this matrix to estimate the data using (10). We have also considered that the noise in general is an additive white Gaussian noise (AWGN) added to the MIMO signals with a variance N which is expressed as:

$$N = \sigma_{shot}^2 + \sigma_{thermal}^2 + \Re^2 P_{rISI}^2 \tag{25}$$

where the third term of (25) has been neglected because of we have assumed LOS scenario only; whereas, the variance of a shot noise is specified by:

$$\sigma_{shot}^2 = 2q\Re^2(P_{rSignal} + P_{rISI})B + 2qI_{bg}I_2B \tag{26}$$

and the variance of thermal noise is given by:

$$\sigma_{thermal}^2 = \frac{8\pi K T_k}{G}\eta A I_2 B^2 + \frac{16\pi^2 K T_k \Gamma}{g_m}\eta^2 A^2 I_3 B^3 \tag{27}$$

where $P_{rSignal}$ is a desired signal power, P_{rISI} is the received power by intersymbol interference and other parameters in (26) and (27) are defined and presented in Table II. In addition,the main parameters of the proposed system are presented in Table II below.

TABLE II: Simulation Parameters

Parameters	Values
Size of room	
Length (m) × width (m) × height (m)	5×5×3
Transmitters	
Number of LED-based transmitters	4
Transmitters Locations	(1.25,1.25),(1.25,3.75), (3.75,1.25),(3.75,3.75)
The LED's semi-angle at half power (FWHM)	70 deg.
Transmitted power per Tx (watt)	10, 100
Optical Receivers	
Number of PD-based receivers	4
The dimensions of the receiver	10 cm × 10 cm
Receiver plane above the floor	0.75 m
Active area (A_R) of receiver	$50\times10^{-6}\ m^2$
Half angle FOV of receiver	70 deg.
Detector orientation: tilt horizontal (elevation)	0 deg.
Detector orientation: tilt vertical (azimuth)	0 deg.
Refractive index of lens at PD	1.5
Transmitted data rate R_B	0.5 Mbps, 1 Mbps
Receiver sensitivity (used with the AD8015 trans-impedance amplifier	-36 dBm
LPF cut-off frequency	$0.7*R_B$
X-Y sweep resolution	0.25 × 0.25 m
Noise parameters values	
Electronic charge (q)	1.60217646×10^{-19}
Equivalent noise bandwidth (B)	R_B [Hz]
Background Current (I_{bg})	$500\times10^{-6}[A]$
Detector responsivity ($\Re$)	0.6
Noise bandwidth factors (I_2, I_3)	$0.562, 0.0868$
Boltzmann's constant (K)	1.38064×10^{-23}
Absolute temperture (T_k)	$313[k]$
Open-loop voltage gain (G)	10
Fixed capacitance of PD (η)	$112[pF.cm^{-2}]$
FET channel noise factor (Γ)	1.5
FET transconductance (g_m)	$30\times10^{-3}[mS]$
PD area (A)	1
Encryption/Decryption	
Encrypted VLC cells size	See Fig. 7
Length of encrypted cell (LEC) (m)	0.5, 1.0, 1.5
The length of encrypted keys (bits)	8, 12, 16
Maximum percentage of unencrypted data (MPUED)	0.05, 0.005, 0.0002

B. *Positioning error distributions*

The proposed 2D indoor positioning system described in Fig. 2 and Fig. 3 is simulated and evaluated using MATLAB. The coordinator generates different location codes based on the positions of transmitters and send them after the full state information (CSI) stage. The receiver consists of has four photodetectors and uses only two of the four signals to recover the location codes and hence determines the locations of the two photodetectors. Therefore, we can calculate the positions of the other two photodetectors based on the size of Rx and the direction of the order of the photodetectors, (i.e. clockwise or anticlockwise as mentioned above). We have also investigated the localization error (The difference between the estimated position and the actual position). In the first approach, the system is considered an ideal system with no noise present at any stage in the aforementioned MIMO VLC system. The results are based on a line-of-sight (LOS) procedure and in the absence of any reflections from wells as shown in Fig. 9 (a). Furthermore, all statistical standards indicate there is a free error in the entire room. In the second approach, we further investigate the case when noise is existing. Here, the same positioning algorithm is applied but with the addition of noise to the received optical signal. The noise is modelled as an additive Gaussian distribution noise over an SNR range of 0 to 30 dB. The selected localization error distributions of the centre of the receiver at 15 dB and 20 dB are shown in Fig. 9 (b), and (c), respectively.

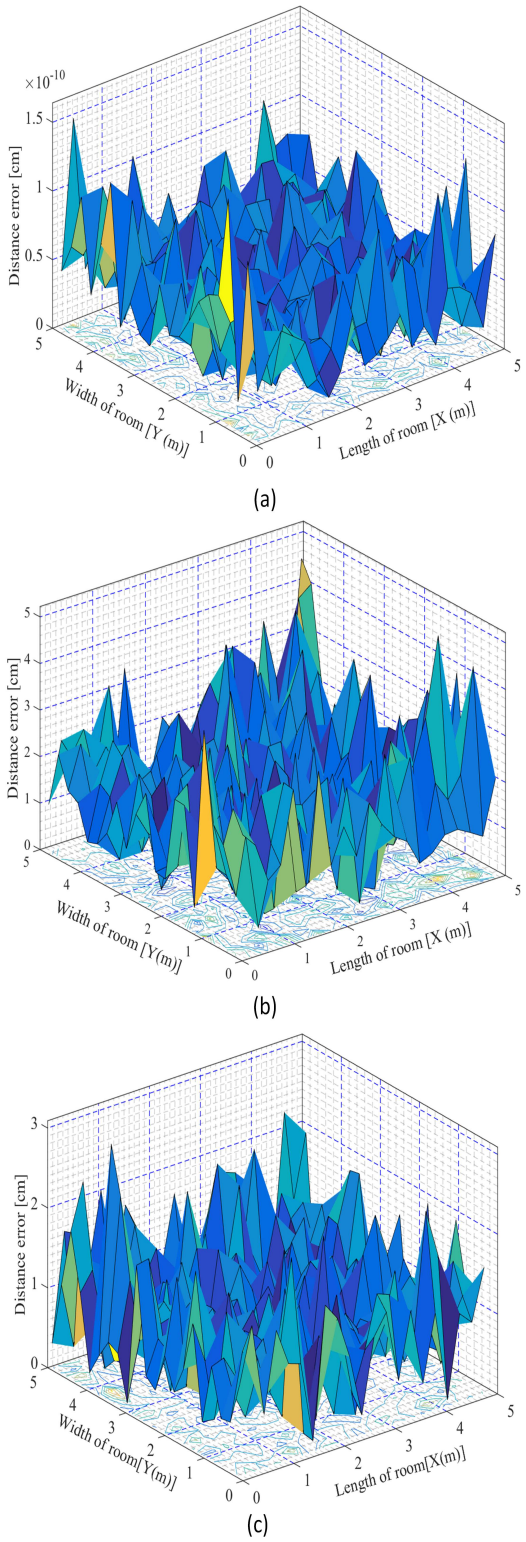


Fig. 9: Spatial distribution of localization error for (a) ideal system (without noise) (b) when SNR = 15 dB (c) when SNR = 20 dB

C. BER distribution for secure MIMO-VLC system

We have also studied the BER distribution of the system using two scenarios. The first scenario is for an ideal system with no added noise. Fig. 10, plots sub-figures of the BER for a typical VLC room. We have tested authorised users for different encrypted VLC cells based on the size of the cell in different places in the VLC room (i.e.; up to 4, 16, and 49 users when LEC = 0.5, 1.0, 1.5 m, respectively). This means that the authorized users (4,16, 49 users) inside the cell have the same centre of the encrypted cell. Thus, they have the same public and private keys. As a result, they can receive the originally transmitted data while all users outside this cell cannot recover the data For instance, in Fig. 10 (a) the centre of encrypted VLC cell is (1.5, 1.5) m so all users nearest to this centre are able to decrypt the data which was sent from the four transmitters for the whole room. Note that the BER is free, but it is capped to 10^{-6} to clarify the difference between the authorised users and unauthorized users outside this cell. The cases in Fig. 10 (b), and (c) are similar to the previous example but with different COECs and different LEC. The second scenario studied is for a MIMO-VLC system with added noise which was modelled as an AWG noise for the wide range but we have selected only when SNR range of 20 dB. Fig. 11 (a) shows the comparison between BER distributions for authorized users inside the encrypted cell and all users outside this cell. Note that BER $\approx 10^{-3}$ for authorized users whereas unauthorized users cannot recover the transmitted data. Other BER distributions are also presented for different COECs and different length of encrypted cell (Fig.11 (b) and (c)) as done in the previous scenario. We have also investigated the BER against a wide range of SNR in three different cases. Firstly, BER against SNR for theoretically single-input-single-output (SISO) VLC system was studied as shown in Fig. 12 (red curve). Secondly, we simulated a SISO-VLC system of four channels. Last of all, a BER in contrast to SNR was simulated for a MIMO-VLC system of four channels as well. In all cases, the receiver's position is in the middle of a standard room Rx's position is (2.5, 2.5) m. This means that the distances are equal between the transmitters and receiver. Note that at BER of 10^{-3} there is more than 3 dB power penalty between the SISO-VLC and MIMO-VLC systems.

VI. Conclusion

In this work, we have designed a new secure MIMO-VLC system using a modified RSA technique to encrypt the transmitted data in the MAC layer based on the location of the user. One of the most important findings to emerge from this study is that the generation of a number of public and private keys with different lengths of keys are enough to distribute them on encrypted VLC cells that have different sizes. In this secure system, the problem of keys distribution has been solved by generating keys in the receiver and send the public key to transmitter only. The ability to control the size of the encrypted VLC cell (LEC) based on the user environment was also demonstrated. Furthermore, no extra data is needed due to the use of the cryptography process, thus maintaining the capacity of the channel. We have also

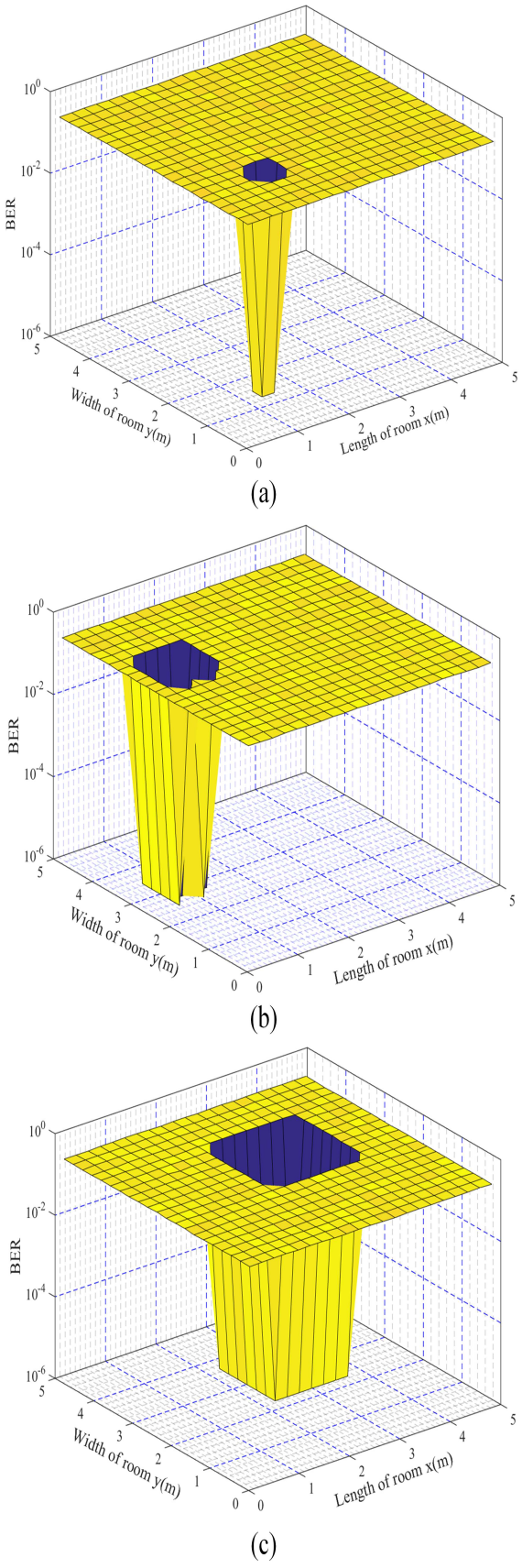


Fig. 10: The BER of an ideal MIMO-VLC system for different encrypted VLC cells when (a) COEC is (1.5, 1.5) m and LEC=0.5m (b) COEC is (1.0, 3.0) m and LEC= 1.0 m (c) COEC is (3.0, 3.0) m and LEC =1.5m.

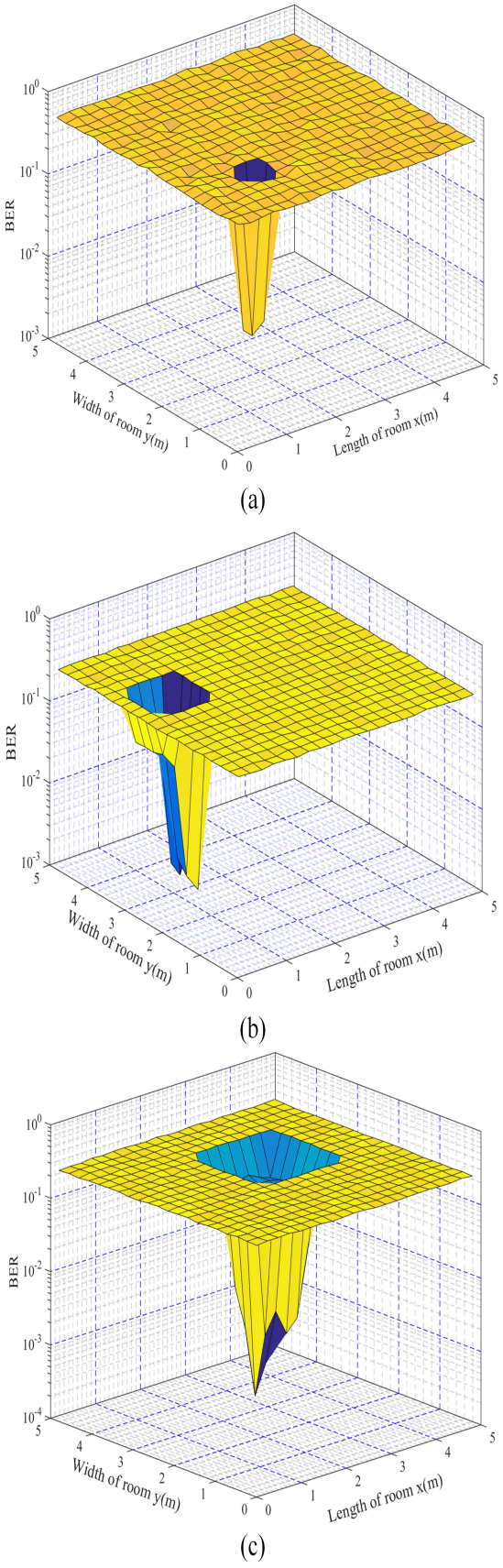


Fig. 11: The BER of an MIMO-VLC system with noise when SNR = 20 dB for different encrypted VLC cells when (a) COEC is (1.5, 1.5) m and LEC=0.5m (b) COEC is (1.0, 3.0) m and LEC= 1.0 m (c) COEC is (3.0, 3.0) m and LEC =1.5m.

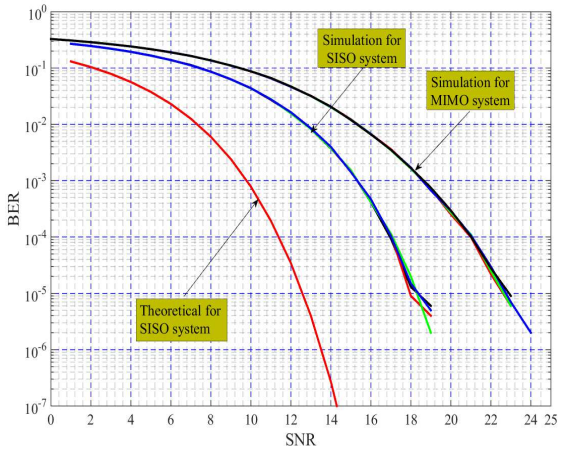


Fig. 12: BER against SNR for a SISO-VLC system (theoretically and simulation) and a MIMO-VLC system (simulation) when the receiver is in the middle of typical room Rx (2.5, 2.5)m

shown that the positioning error was less than 5 cm when SNR=15 dB and have studied the distance error in both ideal and noisy conditions. Moreover, the paper has also presented a study on the BER distribution for authorized users in the encrypted VLC cell and unauthorized users (or eavesdropper) both in an ideal condition and when SNR = 20 dB. Finally, we investigated BER vs SNR for SISO-VLC and MIMO-VLC systems, which showed that the proposed system is working as expected.

VII. Acknowledgments

This research is supported by Northumbria University, UK, Azzaytuna University, Libya, and the Ministry of Higher Education of Libya.

References

[1] S. Dimitrov and H. Haas, *Principles of LED Light Communications Towards Networked Li-Fi*, Cambridge University Press, 1st ed., 2015.

[2] Y. Tanaka, S. Haruyama, and M. Nakagawa, "Wireless optical transmissions with white colored LED for wireless home links", in The 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications,PIMRC, vol.2, pp. 1325-1329, 2000.

[3] K. Hyun-Seung, K. Deok-Rae, Y. Se-Hoon, S. Yong-Hwan, and H. Sang-Kook, "Indoor positioning system based on carrier allocation visible light communication", in *Lasers and Electro-Optics & Quantum Electronics Conference (CLEO/IQEC/PACIFIC RIM)*, pp. 787-789, 2011.

[4] L.-M. Hoa, D. O'Brien, G. Faulkner, Z. Lubin, L. Kyungwoo, J. Daekwang, et al., "100-Mb/s NRZ Visible Light Communications Using a Postequalized White LED", on *IEEE Photonics Technology Letters*, vol. 21, pp. 1063-1065, 2009.

[5] H. Le-Minh, Z. Ghassemlooy, A. Burton, F. Mousa, S. Biswas, P. Anh Tuan, et al., "Self-correcting MIMO visible light communications system using localization," in IEEE International Conference on Communication Workshop (ICCW), pp. 1362-1367, 2015.

[6] Z. Lubin, D. O'Brien, M. Hoa, G. Faulkner, L. Kyungwoo, and J. Daekwang, "High data rate multiple input multiple output (MIMO) optical wireless communications using white led lighting", *IEEE Journal Selected Areas in Communications*, vol. 27, pp. 1654-1662, 2009.

[7] A. H. Azhar, T. Tran, and D. O'Brien, "A Gigabit/s Indoor Wireless Transmission Using MIMO-OFDM Visible-Light Communications", *IEEE Photonics Technology Letters*, vol. 25, pp. 171-174, 2013.

[8] S. Zvanovec, P. Chvojka, P. A. Haigh, and Z. Ghassemlooy, "Visible Light Communications towards 5G", *RADIO ENGINEERING*, vol. 24, p. 9, APRIL 2015.

[9] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights", I*EEE Transactions on Consumer Electronics*, vol. 50, pp. 100-107, 2004.

[10] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications - System and Channel Modelling with Matlab*,: CRC publisher, August 2012.

[11] K. D. Kulat and Deepali Shalke, "performance analysis of ZF and MMSE receiver Algorithm", *International Journal of Research in Engineering and Applied Sciences*, vol. 03, p. 10, Jan 2015.

[12] N. Kaur and L. Kansal, "Performance Comparison of MIMO Systems over AWGN and Rician Channels with Zero Forcing Receivers", *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 5, p. 12, February 2013.

[13] S. Adnan, N. U. Rehman, M. I. Zahoor, "Effect of Different Modulation Techniques Comparison of Linear MIMO Receivers", *International Journal of Computer Applications*, vol. 121, p. 5, July 2015.

[14] Nah, J. H. Y., Parthiban, R., and Jaward, M. H. "Visible Light Communications localization using TDOA-based coherent heterodyne detection", in *IEEE 4th International Conference on Photonics (ICP)*, pp. 247-249, 2013.

[15] T. Nguyen and Y. M. Jang, "Highly Accurate Indoor Three-Dimensional Localization Technique in Visible Light Communication Systems", http://dx.doi.org/10.7840/kics.2013.38C.9.775, vol. 38C, p. 6, 2013.

[16] G. B. Prince and T. D. C. Little, "A two phase hybrid RSS/AoA algorithm for indoor device localization using visible light", in *IEEE Global Communications Conference (GLOBECOM)*, pp. 3347-3352, 2012.

[17] T. Q. Wang, Y. A. Sekercioglu, A. Neild, and J. Armstrong, "Position Accuracy of Time-of-Arrival Based Ranging Using Visible Light With Application in Indoor Localization Systems", *Journal of Lightwave Technology*, , vol. 31, pp. 3302-3308, 2013.

[18] G. Cossu, M. Presi, R. Corsini, P. Choudhury, A. M. Khalid, and E. Ciaramella, "A Visible Light localization aided Optical Wireless system," in *IEEE GLOBECOM Workshops (GC Wkshps)*, pp. 802-807, 2011.

[19] W. Ren and Z. Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication," in 2010 Second International Conference on Modeling, Simulation and Visualization Methods, pp. 221-225, 2010.

[20] S. Sharma, P. Sharma, and R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," in 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), pp. 457-461, 2011.

[21] R. Patidar and R. Bhartiya, "Modified RSA cryptosystem based on offline storage and prime number," in 2013 IEEE International Conference on Computational Intelligence and Computing Research, 2013, pp. 1-6.

[22] A. Al Hasib and A. A. M. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", in *Third International Conference on Convergence and Hybrid Information Technology, ICCIT*, pp. 505-510, 2008.

[23] N. Muhammad, J. M. Zain, and M. Y. Mohd Saman, "Loop-based RSA key generation algorithm using string identity", in *13th International Conference on Control, Automation and Systems (ICCAS)*, pp.255-258, 2013.

[24] O. O. Khalifa, M. D. R. Islam, S. Khan, and M. S. Shebani, "Communications cryptography", in *RF and Microwave Conference (IEEE Cat. No.04EX924)*, pp. 220-223, 2004.

[25] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*: CRC Press, Inc., 1996.

[26] D. R. Stinson, *Cryptography: theory and practice*, 2nd ed ed. London: Chapman: Boca Raton, Fla., 1995.

[27] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5 edition ed.: Prentice Hall, 2010.

[28] Farag I. K. Mousa, H. Le-Minh, Z. Ghassemlooy, X. Dai, S. T. Tran, A. C. Boucouvalas, et al., "Indoor localization system utilizing two visible light emitting diodes", *Optical Engineering*, vol. 55, pp. 116114-116114, 2016.

[29] S. Yamaguchi, V. V. Mai, T. C. Thang, and A. T. Pham, "Design and performance evaluation of VLC indoor positioning system using optical orthogonal codes," in *IEEE Fifth International Conference on Communications and Electronics (ICCE)*, pp. 54-59, 2014.

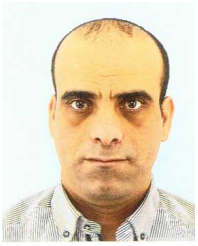
[30] F. Mousa, S. Tran The, A. Burton, M. Hoa Le, Z. Ghassemlooy, T. Q. Duong, et al., "Investigation of data encryption impact on broadcasting visible light communications", in 9th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), pp. 390-394, 2014.

[31] C. H. Lin, S. H. Tsai, and Y. P. Lin, "Secure MIMO transmission via compressive sensing", in *IEEE International Conference on Communications (ICC)*, pp. 7383-7387, 2015.

[32] E. Poonguzhali, A. Priyadarsini, P. Magnifique, and S. Asvini, "A security model for timing attack in cloud environment", in *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-5, 2015.

[33] H. Dahui and D. Zhiguo, "An improved Kerberos protocol based on fast RSA algorithm," in *IEEE International Conference on Information Theory and Information Security*, pp. 274-278, 2010.

[34] B. Lynn Margaret, "The RSA Scheme", in *Public Key Cryptography:Applications and Attacks*, ed: Wiley-IEEE Press, pp. 59-79, 2013.



Farag I. K. Mousa received BSc degree in Electrical & Computer Engineering from Nasser University, Al-khums, and MSc degree in Communication & Waves from the high Studies Academy, Tripoli, Libya in 2001 and 2008 respectively. He was a lecturer in Nasser University for four years. He is currently working toward the PhD degree and Studying positioning and cryptography in visible light communication (VLC) system at Northumbria University, UK.

Noor Al Maadeed is an assistant professor at the computer science and Engineering Department at Qatar University. In 2014 she receive her PhD in in computer science and engineering from Brunel University. She graduate from the Qatar Leadership Centre, first batch 2013. She has been a Lecturer of Computer Engineering in Qatar University since 2001. Her areas of research are speech signal detection, speaker identification and audio/visual speaker recognition. Honours and Awards Qatar Education Excellence Day Platinum Award - New PhD Holders Category 2014-2015.

Krishna Busawon is a Professor in Control Systems Engineering is currently the head of Nonlinear Control research group in the Faculty of Engineering and Environment. He obtained his MPhil and PhD degree in Control Systems Engineering in 1992 and 1996 respectively. After his PhD he was appointed as a Research Fellow at Simon Fraser University in 1997. He then joined the University of Nuevo Len in Mexico where he worked as a Lecturer in the Department of Mechanical and Electrical Engineering (FIME) at Northumbria University, UK. His recent research interests are in chaos and optical wireless communications, hybrid systems and in the area of mathematical modelling, nonlinear control and estimation. He is currently the principal investigator of number of PhD students.

Ahmed Bouridane received an Ingenieur dEtat degree in electronics from Ecole Nationale Polytechnique of Algiers (ENPA), Algeria, in 1982, an M.Phil. degree in electrical engineering (VLSI design for signal processing) from the University of Newcastle-Upon-Tyne, UK, in 1988, and an Ph.D. degree in electrical engineering (computer vision) from the University of Nottingham, UK, in 1992. From 1992 to 1994, he worked as a Research Developer in tele surveillance and access control applications. In 1994, he joined Queens University Belfast, Belfast, UK, initially as Lecturer in computer architecture and image processing and later on he was promoted to Reader in Computer Science. He is now a full Professor in Image Engineering and Security and leads the Computer and Electronic Security Systems Group at Northumbria University at Newcastle, UK, and his research interests are in imaging for forensics and security, biometrics, homeland security, image/video watermarking, cryptography and mobile and visual computing. He has authored and co-authored more than 350 publications and one research book on imaging for forensics and security. Prof Bouridane is a Senior Member of IEEE.

Dr Richard Binns is the Head of Department of Mathematics Physics and Electrical Engineering at Northumbria University. He is currently responsible for a department of 50 staff a member of the faculty executive routinely headed up professional body accreditations and establishing collaborative links to institutions in Malaysia, Singapore, and China. Dr Richard Binns graduated from Huddersfield University with a degree in Electronic and Information Engineering in 1993 and also a Ph.D. in Analogue Test strategies in 1997. He moved to Northumbria University in 2001 on an EPSRC post-doctoral contract looking into Analogue Synthesis tool development in collaboration with Ericson Components and Cadence Design Systems. Current research works are varied from the design of electronics for visible light communications, energy management in electric vehicles, research into radiation detection mechanisms for personal dosimetry and power control systems development.